

CLAIMS

What is claimed is:

1. A method for enciphering an information sequence for subsequent transmission comprising:

5 creating an original message by adding one or more bits to said information sequence;

comparing a numerical value of said original message to a predetermined value;

if the numerical value of said original message is equal to or greater than

10 said predetermined value, changing at least one bit in said original message to obtain a modified message having a numerical value less than said predetermined value; and

encrypting said modified message with a key associated with a first modulus.

15 2. The method of claim 1 wherein creating an original message by adding one or more bits to said information sequence comprises adding a redundant bit to said information sequence at a most significant bit position.

20 3. The method of claim 2 wherein changing at least one bit in said original message to obtain a modified message having a numerical value less than said predetermined value comprises changing said redundant bit at said most significant bit position.

4. The method of claim 1 wherein comparing a numerical value of said original message to a predetermined value comprises comparing said numerical value of said original message to said first modulus.

5 5. The method of claim 4 wherein changing at least one redundant bit in said original message to obtain a modified message having a numerical value less than said predetermined value comprises changing at least one bit in said original message such that the numerical value of said modified message is less than said first modulus.

10

6. The method of claim 1 wherein creating an original message by adding one or more bits to said information sequence comprises adding one or more error detection bits to said information sequence.

15 7. The method of claim 6 wherein adding one or more error detection bits to said information sequence comprises computing a cyclic redundancy check code and appending said cyclic redundancy check code to said information sequence.

20 8. The method of claim 1 wherein encrypting said modified message with a key associated with a first modulus comprises encrypting said modified message with a private key based on said first modulus to obtain a signed modified message.

9. The method of claim 8 further comprising encrypting said signed modified message with a key associated with a second modulus less than said first modulus to obtain an encrypted modified message.

5 10. The method of claim 9 further comprising deciphering said encrypted modified message to obtain a first estimate of said modified message.

11. The method of claim 10 further comprising validating said first estimate of said modified message.

10 12. The method of claim 11 wherein validating said first estimate of said modified message comprises:

error decoding said first estimate of said modified message using said error detection bits to generate an error indication;

15 if said error indication indicates no error, accepting said first estimate of said modified message as a reproduction of said original message;

if said error indication indicates an error, altering at least one predetermined bit in said first estimate of said modified message to obtain a modified estimate of said modified message; and

20 validating said modified estimate of said modified message.

13. The method of claim 12 wherein validating said modified estimate of said modified message comprises performing a bit alteration check to determine whether a predetermined bit of said modified message is an altered bit.

5 14. The method of claim 13 wherein performing a bit alteration check to determine whether a predetermined bit of said modified message is an altered bit comprises:

determining whether bit errors occurred in said at least one predetermined bit;

10 if bit errors occurred in said at least one predetermined bit, determining whether the value of said at least one predetermined bit has an expected value; and

if said at least one predetermined bit has an expected value, determining whether said modified estimate of said modified message has an

15 expected value.

15. The method of claim 14 wherein determining whether bit errors occurred in said at least one predetermined bit comprises determining whether a bit error occurred in a most significant bit.

20 16. The method of claim 15 wherein determining whether the value of said at least one predetermined bit has an expected value comprises determining whether said most significant bit is equal to zero.

17. The method of claim 16 wherein determining whether said modified estimate of said modified message has an expected value comprises determining whether said modified estimate with said most significant bit position equal to one is greater
5 than or equal to said encryption modulus.

18. A method of encrypting a message comprising the steps of:
forming an original message by appending one or more redundant bits to an
information sequence;
10 comparing a value of said original message with a value of a first modulus
and modifying said original message to obtain a modified message if
said original message is greater than or equal to said first modulus;
signing said modified message with a first key based on said first modulus to
form a signed message;
15 encrypting said signed message with a second key based on a second
modulus to form a doubly encrypted message; and
sending said doubly encrypted message to a recipient.

19. The method of claim 18 wherein forming an original message by appending
20 one or more redundant bits to an information sequence comprises forming a
message having a length equal to said first modulus.

20. The method of claim 18 wherein signing said modified message with a first key based on said first modulus to form a signed message comprises signing said modified message with a sender's private key.

5 21. The method of claim 18 wherein modifying said original message to obtain a modified message if said original message is greater than or equal to said modulus comprises changing the value of one of said redundant bits.

22. The method of claim 18 wherein forming an original message by appending 10 one or more redundant bits to an information sequence comprises adding error detection bits computed on said information sequence to said information sequence.

23. A method of deciphering a doubly encrypted bitstring comprising:
15 deciphering said doubly encrypted bitstring to obtain a once encrypted bitstring;
deciphering said once encrypted bitstring to obtain a first estimate of a plaintext message having one or more error detection bits;
decoding said first estimate of said plaintext message to produce an error 20 indication;
if said error indication indicates an error, performing a bit alteration check to determine whether a predetermined bit in said first estimate of said plaintext message was altered.

24. The method of claim 23 wherein performing a bit alteration check to determine whether a predetermined bit in said first estimate of said plaintext message was altered comprises altering a predetermined bit in said first estimate of 5 said plaintext message to generate a modified plaintext message and testing the validity of said modified plaintext message.

25. The method of claim 23 wherein performing a bit alteration check to determine whether a predetermined bit in said first estimate of said plaintext 10 message was altered comprises checking said first estimate of said plaintext message for a bit error in a predetermined bit position.

26. The method of claim 25 wherein performing a bit alteration check to determine whether a predetermined bit in said first estimate of said plaintext 15 message was altered further comprises determining a value of a bit in said predetermined bit position.

27. The method of claim 26 wherein performing a bit alteration check to determine whether a predetermined bit in said first estimate of said plaintext 20 message was altered further comprises altering said value of said bit in said predetermined bit position to obtain a modified estimate of said plaintext message and comparing a value of said modified estimate of said plaintext message to a predetermined value.

28. The method of claim 23 further comprising:

modifying said once encrypted bitstring if said bit error check produces an
error;

5 deciphering said modified once encrypted bitstring to obtain a second
estimate of said plaintext message;

decoding said second estimate of said plaintext message to produce an error
indication;

if said error indication indicates an error, performing a bit alteration check to
10 determine whether a predetermined bit in said second estimate of said
plaintext message was altered.

29. The method of claim 28 wherein modifying said once encrypted bitstring if
said bit error check produces an error comprises adding a predetermined value to
15 said once encrypted bitstring.

30. The method of claim 29 wherein adding a predetermined value to said once
encrypted bitstring comprises adding a value equal to a modulus associated with an
encryption key used to generate said doubly encrypted bitstring.

31. A method of deciphering a doubly encrypted bitstring comprising:
deciphering said doubly encrypted bitstring to obtain a once encrypted
bitstring;
5 modifying said once encrypted bitstring by adding an integer multiple of a
modulus associated with an encryption key used to generate said doubly
encrypted bitstring to said once encrypted bitstring to obtain a modified
once-encrypted bitstring;
deciphering said modified once encrypted bitstring to obtain an estimate of
10 said plaintext message.

32. The method of claim 31 further comprising decoding said estimate of said
plaintext message to produce an error indication.

15 33. The method of claim 32 further comprising performing a bit alteration check
to determine whether a predetermined bit in said estimate of said plaintext message
is an altered bit, if said error indication indicates an error.

34. An encryption device comprising:

an error encoder to produce an encoded message having one or more error detection bits, wherein said error encoder alters a predetermined bit in said encoded message to produce a modified message when a value of said encoded message is greater than or equal to a predetermined value;

5 and

a cryptographic processor to encrypt said modified message to obtain an encrypted message.

10 35. The encryption device of claim 34 wherein said cryptographic processor encrypts said modified message using a first encryption key associated with a first modulus.

15 36. The encryption device of claim 35 wherein said first encryption key is a private key of a sender of said message.

20 37. The encryption device of claim 35 wherein said cryptographic processor further encrypts said modified message using a second encryption key associated with a second modulus, wherein said second modulus is different from said first modulus.

38. The encryption device of claim 37 wherein said second encryption key is a public key of a recipient of said message.

39. The encryption device of claim 35 wherein said first predetermined value is equal to said first modulus less one.

5 40. The encryption device of claim 35 wherein said encoder outputs said encoded message unmodified when said value of said encoded message is less than said predetermined value.

41. The encryption device of claim 35 further comprising a transmitter for sending said encrypted message to a recipient.

10

42. A device for decrypting data comprising:
a cryptographic processor to decipher a doubly encrypted bitstring to obtain a first estimate of a plaintext message, wherein said cryptographic processor uses a first key associated with a first modulus for a first decryption operation and a second key associated with a second modulus for a second decryption operation; and
a decoder to decode said first estimate of said plaintext message and to generate an error indication, said decoder comprising a bit alteration detector to determine whether a predetermined bit in said first estimate of said plaintext was altered.

15

20

43. The device of claim 42 wherein said bit alteration detector alters a predetermined bit in said first estimate of said plaintext message to generate a modified plaintext message and tests the validity of said modified plaintext message.

5

44. The device of claim 42 wherein said bit alteration detector checks said first estimate of said plaintext message for a bit error in a predetermined bit position.

45. The device of claim 44 wherein said bit alteration detector determines a 10 value of a bit in said predetermined bit position.

46. The device of claim 45 wherein said bit alteration detector alters the value of said bit in said predetermined bit position to obtain a first modified estimate of said plaintext message and compares a value of said first modified estimate of said 15 plaintext message to a predetermined value.

47. The device of claim 42 wherein said cryptographic processor modifies said once encrypted bitstring in response to an error indication from said bit alteration detector to obtain a modified once encrypted bitstring and decodes said modified 20 once encrypted bitstring to obtain a second estimate of said plaintext message.

48. The device of claim 47 wherein said decoder decodes said second estimate of said plaintext message and generates an error indication.

49. The device of claim 48 wherein said bit alteration detector determines whether a predetermined bit in said second estimate of said plaintext was altered.